

ADP SECURITY POLICY

- Section I. Policy
II. Purpose
III. Definitions
IV. Scope
V. Guidance
VI. Background
VII. Objectives
VIII. Responsibilities
IX. Procedures

I. POLICY

It is policy of the Centers for Disease Control (CDC)* that all agency personnel who are responsible for the use of ADP equipment take appropriate actions to prevent loss or misuse of the hardware, software, and associated data. Responsible individuals include users, users' supervisors, agency officials, and ADP System Security Officers. The extent of the action taken by the user and supervisory staff should be commensurate with the criticality, sensitivity, and value of the hardware, software, and data.

II. PURPOSE

The purpose of this policy issuance is:

- To establish responsibilities and provide guidance for the identification and correction of vulnerabilities associated with ADP security at CDC.
- To prevent or minimize common problems that limit computing usefulness.

III. DEFINITIONS

ADP Equipment: Any machine used for data or text processing functions. This includes word processing equipment, microcomputers, minicomputers and mainframe computers, as well as any associated peripheral devices.

ADP Systems Security Officer (SSO): Information Resources Management

Office (IRMO) or Center/Institute/Program Office (CIO) official designated to be responsible for developing, coordinating, managing, and evaluating CDC's automatic data processing (ADP) security programs for CDC or the respective organizational component.

ADP Workstation: An individual terminal, microcomputer, or other device which performs data or text processing functions on a stand-alone basis or through connection (direct or indirect via telecommunications) to a mainframe, mini- or microcomputer.

Backup: The creation of duplicate data and software files. Copyright laws must be adhered to when copying software.

Clearance (Personnel): OMB Circular A-130 Appendix III, the Office of Personnel Management, and the HHS Information Resources Management (IRM) Manual, Part 6 require that each agency ensure that individuals who have access to or use computers or computer-related assets obtain appropriate clearances.

Computer Virus: Computer programs that are written to "infect" other computer programs, systems, or data and cause disruption of the normal system operation or destruction of data.

Contingency Plan: A documented description of actions and procedures that will be used before, during, and after an event which prevents normal operations.

Critical Information System: An application system which accomplishes tasks crucial to the organization's operation and mission.

Delete (File): A procedure employed to remove a file from a disk. However, particularly with microcomputers, this only modifies the disk directory and the file may still be accessible. To render a file inaccessible the data must be written over. See Write-Over below.

Documentation: A set of written reference material which describes an application, a procedure, or a process.

Encryption: A cryptographic method used to prevent unauthorized disclosure of data by scrambling sensitive and confidential data through the use of algorithms and keys.

Misuse: Any action which would result in fraud, waste, or abuse of ADP equipment, applications, or data.

Password: A secret code comprised of letters and/or numbers granted to, or established by, an individual to gain specific access to automated data and software, and to bar access to unauthorized individuals.

Power Surge/Spike: A transient fluctuation of power which can have unpredictable and undesirable results, such as damaging equipment or creating erroneous data. Microcomputers are particularly vulnerable to this risk.

Risk Analysis: An assessment to quantify potential misuse or loss.

Sensitive Data: Data, which by its very nature, requires a degree of protection (e.g., Privacy Act data, proprietary data, privileged data).

Telecommunications: The communication of data or text by electronic means over telephone or other lines.

Vulnerability: The susceptibility to the risk of misuse or loss.

Write-Over: The placement of meaningless characters into data fields to render a file inaccessible.

IV. SCOPE

This issuance is applicable to all ADP hardware, software, and associated data at CDC. It is also applicable to ADP hardware, software, and associated data used by any organization in support of work on CDC contracts, grants, and cooperative agreements. This issuance also applies to ADP equipment, software, and data which is taken home to perform agency work. It specifically includes all mainframe computers, minicomputers, microcomputers and word processing equipment, and the software and data processed by any ADP equipment.

V. GUIDANCE

These requirements are primarily based on the minimum security requirements defined in the HHS IRM Manual, Part 6, but also include requirements specified in National Bureau of Standards Guidelines, OMB Circular A-130, and National Security Decision Directive 145.

Additional policy guidance is provided in other Information Resources Management policies.

Additional technical guidance can be obtained from equipment and software manufacturer's specifications and the CDC ADP User's Guide, the

CDC Microcomputer Standards, and the Guidelines on Microcomputer Acquisition and Use at CDC.

VI. BACKGROUND

The mainframe computer was the principal source of computing resources for most users until the introduction of microcomputers into the office environment. Now users have a wide array of decentralized computer equipment available to them, including text processors, microcomputers and minicomputers. Most ADP workstations now include powerful computer chips, large quantities of local storage, and sophisticated processing capabilities. This tremendous increase in the computing power and data storage capabilities of small computers requires that they also now receive serious attention in the area of ADP security. The concepts of ADP security are applicable to all types of ADP equipment, although the specific procedures that need to be implemented will vary depending upon the specific circumstances.

Physical security, for example, is one aspect of ADP security that now requires the attention of users. CDC's mainframe computer is housed in a special facility behind locked doors, with its own environmental controls such as air conditioning, fire-fighting equipment, electrical power sources and backup power supply. Any related physical security problems are handled by a few individuals trained in security. But with the placement of ADP equipment into the office environment, many of the physical security concerns associated with the mainframe computer are now also pertinent to this equipment in the office. Controlling physical access by unauthorized users to ADP workstations can be a difficult problem to solve because one of the major benefits is their easy accessibility. Protecting this equipment from theft and physical damage is not different from protecting office equipment such as calculators or typewriters. In addition, microcomputers are particularly vulnerable to fluctuations in electrical power and may require special protection.

Of potentially far greater importance than physical security, however, is the protection and safeguarding of data and software from loss and misuse, regardless of the type of computer or text processor used.

Since CDC is a civilian agency where the large majority of our ADP hardware and software are noncritical and the data are nonsensitive, cost-effectiveness and efficiency are the major focus. Section IX of this document presents a list of specific action items that can help avoid potential security problems.

VII. OBJECTIVES

The overall objective of this policy is to maximize the security of CDC's ADP equipment and associated software and data by assuring integrity and minimizing the potential for loss or misuse.

The policy also attempts to serve an educational role for users, supervisors, and other CDC officials in protecting CDC resources from unintentional loss through improper or inadvertent actions.

VIII. RESPONSIBILITIES

A. Users and Supervisors

All users of ADP equipment, unless otherwise specified, are responsible for carrying out the security requirements in this issuance and are responsible for preventing loss or misuse of this equipment and associated software and data. Supervisors and organizational property officers are responsible for ensuring that the required actions are performed.

B. ADP Systems Security Officers

The CDC ADP Systems Security Officer (SSO) and Center/Institute/ Program Office (CIO) ADP Systems Security Officers (SSO's) are responsible for ensuring compliance with and providing training and consultation on security requirements specified in this issuance. The CDC ADP SSO will provide overall coordination for ADP security operations at CDC.

C. Privacy Act Officer and Coordinators

The CDC Privacy Act Coordinator and CIO Privacy Act Liaisons are responsible for providing consultation to ensure that the ADP security safeguards for a Privacy Act system of records are consistent with the safeguards described in the Federal Register notice covering the respective system of records.

D. Office of Program Support

The Office of Program Support is responsible for CDC's physical security program including ensuring compliance with physical security requirements and providing technical consultation on physical security measures related to ADP.

IX. PROCEDURES

Every effort should be made to identify potential problems and establish

operating procedures to minimize ADP security risks and otherwise enhance productivity. The following 20 areas address basic physical, technical, and administrative considerations necessary to protect the equipment, software, and data. Applicability of each procedure depends on the type and use of the ADP equipment. Additional specific requirements and guidance on mainframe data security can be found in the CDC ADP User's Guide. The following procedures are grouped into categories that address data, physical, personnel, and assessment/planning concerns.

Data

(1) Classified Information and Data: Classified information and data are subject to special security measures.

Action: Classified information and data shall not be stored, processed, or transmitted on nonsecure equipment. Consult with the CDC Communications Center regarding classified information.

(2) Backup (Data or Text Files): Storage of data or text files in a single place substantially increases the risk of data loss inadvertently or intentionally, e.g., computer viruses. Data and text files should be protected by duplication and remote storage.

Action: On a periodic and systematic basis, backup (copy or file) data and text files on media stored in a remote location. Assure that the backup is successful by accessing the backup files before storing them away in a separate location. Consider storage in secure facilities (locked cabinets, safes, etc.) depending upon the criticality, sensitivity, and value of the data. When appropriate, evaluate the value of uploading microcomputer data sets for storage on CDC's mainframe. Large data sets that are critical or expensive to reconstruct are prime candidates for mainframe storage.

Mainframe data sets stored on disks are automatically backed up by IRMO staff. Tapes, however, are not backed up by IRMO and are the responsibility of the user. Procedures and facilities are available for users to copy tape data sets and request off-site secure storage. Contact the Computer Center when such action is required.

(3) Backup (Software): Similar risks of data and text file loss or misuse apply to operating software and user-written programs stored in only one place, e.g., solely on micro- or minicomputer internal memory or on a single floppy disk.

Data (Continued)

Action: Create backup copies of user-written programs, including items such as spreadsheet templates. Also, where authorized by copyright law and software licensing agreements, create a backup copy of your off-the-shelf software. After creating the backup copy on a diskette, place a "write-protect" tab over the notch on the backup copy. Use the backup copy as your operational software, and store the original copy in a safe place. Do not copy or allow others to make copies of the software when such copying is specifically forbidden by copyright or software licensing agreement. Given the substantial investment of personnel time in developing user-written programs, take similar steps to protect all programs developed in-house.

(4) Documentation: Documentation is written reference material used to describe and define a software package or system. It usually includes a description of the package or system and detailed operating instructions. It is important to keep up-to-date documentation so that the software can be utilized effectively, efficiently, and correctly. In many cases it may be appropriate to describe the particular design of a software application.

Action: Maintain and protect a complete and current set of documentation for all system, user, and off-the-shelf software. It is especially important to document user-written applications, particularly those in a production environment and those which are critical or handle sensitive data.

(5) Data Communications: Users should maintain control over data communications to assure integrity and security of data.

Action: Users should verify that the proper connection has been made before transmitting or receiving data via telecommunications. Whenever feasible, data should be communicated using error checking data transfer protocols.

(6) Data Control: Control procedures for data should be in place to prevent loss of data and unauthorized access. Additionally, the growing threat of computer viruses warrants controls on the source of data including software and data files.

Action: Install procedures to ensure proper handling of data, e.g., provide labels which clearly identify reports, and use labels on diskettes and tapes that identify individual files.

Obtain software and data from reliable sources only. Do not incorporate unknown public domain or bulletin board software on any computer system since the virus can be very difficult to detect and can surface at any future time causing substantial damage. For critical systems, consider obtaining legitimately marketed virus identification or vaccination programs.

(7) Data Access: Data is an agency asset which has value; therefore, it needs to be protected from unauthorized access, misuse, alteration, loss, or destruction. The more sensitive or critical the data, the greater the need to install protection devices and systems. In some instances, there is a need to restrict access to sensitive data based on a "need-to-know" basis. Examples of sensitive data are patient data, prerelease budget information, preaward grant data, contract information, and information containing personal identifiers. A request for access from individuals or establishments outside the agency should be handled in accordance with Freedom of Information Act (FOIA) provisions. The CDC FOIA Officer should be consulted for guidance in handling specific requests.

Action: The user and supervisor should assess the sensitivity, criticality, value, cost, confidentiality, etc., of the data maintained. Based on such assessment, security features such as password protection (routinely changed), audit trails, encryption, locking devices on microcomputers, or other protection should be installed and used to prevent unauthorized access to appropriate systems and data. Contact your SSO for assistance.

(8) Disposition of Reports and Data: Data files and reports which contain sensitive or confidential data should receive proper disposition. Depending on the sensitivity, erase (write-over) unneeded data from storage media. This will render the data inaccessible and unusable. Specific data fields containing sensitive or confidential information, such as personal identifiers, should be removed from active records as soon as they are no longer needed.

Action: Reports containing sensitive or confidential data must be shredded. Write over any unneeded sensitive or confidential data files on hard disks and diskettes. Simply deleting microcomputer files only alters the disk directory and still allows files to be retrievable.

(9) Storage of Reports and Data: Sensitive or confidential reports and data should be protected from unauthorized access.

Action: Sensitive or confidential reports and data on diskettes or tapes

should be stored in a lockable file cabinet or desk when not in use. Diskettes should be removed from the machine, placed in the jacket, and put in a safe place. Diskettes should not be exposed to contaminants such as coffee spills and cigarette smoke, or sources of magnetism such as workstation monitors and telephones.

(10) Privacy Act and Other Sensitive Data: The Privacy Act of 1974 requires that record system data routinely retrieved by the name of the individual or by some identifying particular, such as Social Security Number, be protected by adequate physical, administrative, and procedural safeguards to ensure the security and confidentiality of the data.

Action: If processing or maintaining data from a Privacy Act system of records on ADP equipment, take additional steps to protect the data. The procedures specified in this issuance are the minimum acceptable procedures for any ADP activities. Privacy Act safeguards are provided in the published Federal Register notice which describes the particular system of records within the CIO. If processing Privacy Act information on ADP equipment, be sure to consult with the Automated Information Systems Security Officer (SSO), as well as the CIO Privacy Act Liaison or the CDC record system manager, to identify and implement additional protective measures. These measures may include:

- a. Restricting access to the files to agency employees with a bona fide "need to know" in order to carry out the duties of their positions or to accomplish the purposes for which the data were collected;
- b. Using a special "certified" process to completely overwrite tapes on the mainframe or overwriting (not merely deleting) microcomputer files;
- c. Safeguarding source documents, printouts or diskettes, by storing them in locked cabinets in locked offices when not in use.

Certain highly sensitive data, such as those collected with an Assurance of Confidentiality, Section 308(d) of the Public Health Service Act, may require even more stringent safeguarding measures than those listed above, such as encryption. The Reports Clearance Officer, FOIA Officer, the CDC Privacy Act Coordinator, and the CDC Systems Security Officer may be consulted for guidance.

Physical

(11) Physical Access: ADP equipment is becoming more and more portable and, therefore, much more susceptible to theft. In addition, the

equipment's most beneficial aspect, ease of use, makes it much easier for unauthorized individuals to view or change data or information.

Action: The user and supervisor should evaluate the need to install devices such as door locks to the room housing the device, cypher locks, and anchor pads which will control access to, or prevent theft of, ADP equipment. If the office is easily accessible by a stairwell, outside door, or first floor window, it is especially vulnerable to theft. ADP equipment located in less secure remote facilities may require additional measures, including special door locks, window bars, and indelible markings on equipment cases. Contact the SSO for assistance.

(12) Electrical Power: Power fluctuations, surges, and spikes may lead to unpredictable and undesirable results such as damage to hardware, creation of erroneous data, or loss of data.

Action: The user and supervisor should evaluate the need for installation of a device which protects the ADP equipment from these events based on the criticality of the system and data and the frequency of occurrence. Protection devices may include surge protectors, static electricity mats or sprays, power conditioners, or uninterruptible power supplies (UPS). Contact IRMO for advice and assistance.

(13) Travel: ADP equipment and data may be subject to unusual hazards while in transit.

Action: Users should protect their equipment and data against extreme fluctuations in environmental conditions, including temperature and humidity. Airport X-ray machines and metal detectors may pose a hazard to data stored on diskettes. As a precaution, duplicate copies of diskettes containing data and software should be made and transported separately from the originals. Metal detectors and X-ray equipment should be avoided. Also, as with all magnetic data storage media, diskettes should be carefully protected against any other sources of magnetism.

Personnel

(14) Individual Responsible for System Security: Individual users and their supervisors have primary responsibility for ADP security.

Action: Users of ADP equipment and their supervisors should become familiar with the requirements of this issuance, and supervisors should assure adherence through periodic review.

(15) Orientation and Training: A user awareness program provides users with an orientation of security problems, responsibilities, and procedures.

Action: The CDC ADP SSO shall conduct periodic security training classes for selected CDC staff. Introductory classes on the use of microcomputers which are taught at CDC will include segments on security. The program will include such topics as backing up files, securing data, instructing users not to perform privileged operations, not smoking or drinking near the workstation, proper use of passwords and access control methods, and the need for securing and protecting data.

(16) Personnel Access: ADP equipment is usually assigned to individuals or multiple users within a defined work area. Access to the equipment should be limited to those individuals specifically authorized in order to protect the equipment, software, and associated data from intentional or unintentional loss or misuse.

Action: It is the user's and supervisor's responsibilities to ensure that only appropriate persons use the ADP equipment within their area of responsibility. This is particularly important where the equipment is easily accessible by numerous individuals, or if the equipment is shared by multiple employees.

(17) Personnel Security: All individuals who use ADP equipment must have the required ADP security clearances. In most cases, only the basic clearance that is performed when an individual enters the Federal service is necessary. However, higher level clearances may be required for individuals involved in classified, sensitive or critical agency systems that utilize ADP equipment.

Action: It is the supervisor's responsibility to ensure that appropriate clearances are obtained. Contact the SSO for further guidance in classifying positions of those individuals who use ADP equipment.

Assessment/Planning

(18) Risk Analysis: The user and/or supervisor are responsible for analyzing the value of assets being protected, the nature and likelihood of threats against the assets, and the cost-effectiveness of existing or proposed safeguards. The analysis should be commensurate with the value of the assets, the sensitivity of the data, and the criticality of the system.

Action: Prior to installation of ADP equipment or within 90 days after installation, the user and/or supervisor should conduct a risk analysis of the equipment, applications, and expected data. This requirement also pertains to major application software systems installed on existing ADP equipment. Update this analysis at least annually. Decisions to install security safeguards should be based on the cost of the safeguard versus the potential loss. Contact the CIO SSO or the CDC SSO to obtain microcomputer software to automate the risk analysis process and evaluation.

(19) Contingency Plan: The user and/or supervisor are responsible for advanced planning to determine the course of action to take in the event the ADP equipment is inoperable for periods of time (e.g., 1 day, 1 week, or longer).

Action: The user and/or supervisor should develop and maintain a contingency plan which covers emergency operations, backup operations, and recovery plans. This requirement is applicable to all ADP equipment, including CDC's mainframe computer. The level of effort and planning should be based on the criticality of the equipment, system, or data maintained. IRMO is responsible for developing contingency plans for CDC's critical operations and applications on the mainframe computer.

(20) Periodic Review: Since the uses of ADP equipment change constantly, security is an ongoing process. As new software applications are installed or existing systems are modified (e.g., new off-the-shelf packages are installed or a new device is added), security needs may change.

Action: The user and/or supervisor should reexamine ADP security when significant changes are made, or at least annually, to determine whether new risks or vulnerabilities have been introduced and what measures should be implemented to eliminate or minimize them. Plan ahead. Ensure that security safeguards and considerations are included in new or modified applications prior to implementation.

*References to CDC also apply to the Agency for Toxic Substances and Disease Registry.